Network Fundamentals, Domain & Hosting Investigation, Public & Private IP Address

Presented by:

ELIAS HOSSEN

Police Inspector (UB)

Digital Forensic Lab

CID HQ, Dhaka.

Network

A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

Network Fundamentals

Network Fundamentals refers to the foundational knowledge and understanding of how computer networks are built, operate, and are used. It covers the basic concepts of networking, including network types, hardware, software, protocols, and common networking terms.

Key Concepts in Network Fundamentals:

- **Network Types:**

Understanding different network types like
LAN (Local Area Network),
WAN (Wide Area Network),
MAN (Metropolitan Area Network), and Internet.

- **Network Hardware:**

Familiarity with essential networking devices such as switches, routers, access points, and wireless access points.

switches https://www.netgear.com/business/wired/switches/
routers https://www.geeksforgeeks.org/introduction-of-a-router/
access points https://www.pynetlabs.com/access-point-and-its-types/
wireless access points
https://www.netgear.com/business/wifi/access-points/

- **Network Protocols:**

Knowledge of protocols like TCP/IP, HTTP, and DNS, which govern how data is transmitted across networks.

TCP/IP https://www.geeksforgeeks.org/tcp-ip-model/
HTTP https://www.geeksforgeeks.org/http-full-form/

DNS https://www.geeksforgeeks.org/domain-name-system-dns-in-application-layer/

- **Network Models:**

Understanding the OSI model and its layers, and the TCP/IP model, which provide frameworks for network communication.

- **Network Security:**

Basic understanding of network security concepts and how to protect networks from threats.

- **Network Troubleshooting:**

Learning basic troubleshooting techniques for common network issues.

- **IP Addressing and Subnetting:**

Understanding IP addresses, how they are assigned, and how to use subnetting to manage network traffic.

Why is Network Fundamentals Important?

- **Foundation for Networking Careers:**

Network fundamentals provide a solid base for those pursuing careers in networking, IT, or cybersecurity.

- **Understanding Network Infrastructure:**

It helps individuals understand how networks work, allowing them to manage and troubleshoot network issues effectively.

- **Security Awareness:**

It helps individuals understand network security concepts and how to protect their own networks and systems.

- **Problem-Solving:**

It equips individuals with the knowledge to diagnose and resolve common network problems.

Domain

A domain name is a string of text that maps to an alphanumeric IP address, used to access a website from client software. In plain English, a domain name is the text that a user types into a browser window to reach a particular website. For instance, the domain name for Google is ‘google.com’.

The actual address of a website is a complex numerical IP address (e.g. 192.0.2.2), but thanks to DNS, users are able to enter human-friendly domain names and be routed to the websites they are looking for. This process is known as a DNS lookup.

Who manages domain names?
Domain names are all managed by domain registries, which delegate the reservation of domain names to registrars. Anyone who wants to create a website can choose a registrar to register a domain name, and there are currently over 300 million registered domain names.

What is the difference between a domain name and a URL?

A uniform resource locator (URL), sometimes called a web address, contains the domain name of a site as well as other information, including the protocol and the path.

For example, in the URL
https://cloudflare.com/learning/

'cloudflare.com' is the domain name,
'https' is the protocol,
'/learning/' is the path to a specific page on the website.

What are the parts of a domain name?

Domain names are typically broken up into two or three parts, each separated by a dot. When read right-to-left, the identifiers in domain names go from most general to most specific. The section to the right of the last dot in a domain name is the top-level domain (TLD). These include the 'generic' TLDs such as '.com', '.net', and '.org', as well as country-specific TLDs like '.uk' and '.jp'.

To the left of the TLD is the second-level domain (2LD) and if there is anything to the left of the 2LD, it is called the third-level domain (3LD). Let's look at a couple of examples:

For Google's US domain name, 'google.com':

- '.com' is the TLD (most general)
- 'google' is the 2LD (most specific)

But for Google UK's domain name, 'google.co.uk':

- '.uk' is the TLD (most general)
- '.co'* is the 2LD
- 'google' is the 3LD (most specific)

**In this case, the 2LD indicates the type of organization that registered the domain (.co in the UK is for sites registered by companies).*

How to keep a domain name secure

Once a domain name has been registered with a registrar, that registrar is in charge of notifying the registrant when their domain is about to expire and giving them the chance to renew, ensuring they do not lose their domain name. In some cases,

registrars will pray on their users' expired domain names by buying those domains the second they expire and then selling them back to the original registrant at an exorbitant price.
It is important to choose an honest and trustworthy registrar like Cloudflare Registrar to avoid these kinds of predatory practices.

Hosting

In simple terms, hosting refers to the service that provides storage space for a website or application on a server on the internet. It allows your website to be accessible to anyone with an internet connection. Hosting providers rent out space on their servers, enabling websites to store their files and become publicly viewable.

Domain vs hosting: Definition and differences

When creating a website, two terms you'll encounter immediately are "domain name" and "web hosting." While both are essential components of any website, they serve completely different purposes.
If you think of your website as a physical house, the domain name (like example.com) would be its street address that people use to visit you.
Web hosting, on the other hand, would be the actual property where your house stands – the land and foundation that supports everything.

Without a domain name, users wouldn't be able to find your website easily. Without hosting, your website wouldn't have anywhere to exist on the internet.

Every functioning website requires both elements working together: a domain name (with an extension like .com, .org, or .net) and a hosting plan where all your website's files, images, and data are stored.

Understanding the key differences between domains and hosting is crucial before you start building your website. This article explains everything you need to know about these essential website components—what they are, how they work together, and what distinguishes them from each other.

Domain & Hosting Investigation

A Domain investigation is used to obtain the IP address the email is sent from and it then verifies it with the ones mentioned in the SPF (Sender Policy Framework) record.

https://smallseotools.com/domain-hosting-checker/

https://dnslytics.com/

https://namechk.com/

https://lookup.icann.org/en

https://www.site24x7.com/tools/domain-expiry.html

https://dnschecker.org/all-tools.php

https://www.nameboy.com/

https://www.isitwp.com/

https://www.networksolutions.com/domains

https://dnschecker.org/

https://mxtoolbox.com/

https://whois.whoisxmlapi.com/bulk-whois-lookup

https://whois.domaintools.com/

IP Address

An Internet Protocol (IP) address is the unique identifying number assigned to every device connected to the internet.

1. **Class A**: 10.0.0.0 and 10.255.255.255
2. **Class B**: 172.16.0.0-172.31.255.255

3. **Class C**: 192.186.0.0-192.168.255.255
4. **Class D:**224.0.0.0 -239.255.255.255
5. **Class E** 240.0.0.0 - 254.255.255.254

Class D or multicast: 224.0.0.0 - 239.255.255.255

Multicast is a method where a single source sends data to multiple recipients simultaneously.

Class E, which are reserved for experimental usage: IP addresses between 240.0.0.0 and 254.255.255.254

Reserved IP Address Summary

Here is a summary of the key reserved IP address ranges and their purposes:

Range	Purpose
10.0.0.0 - 10.255.255.255	Private networks (Class A)

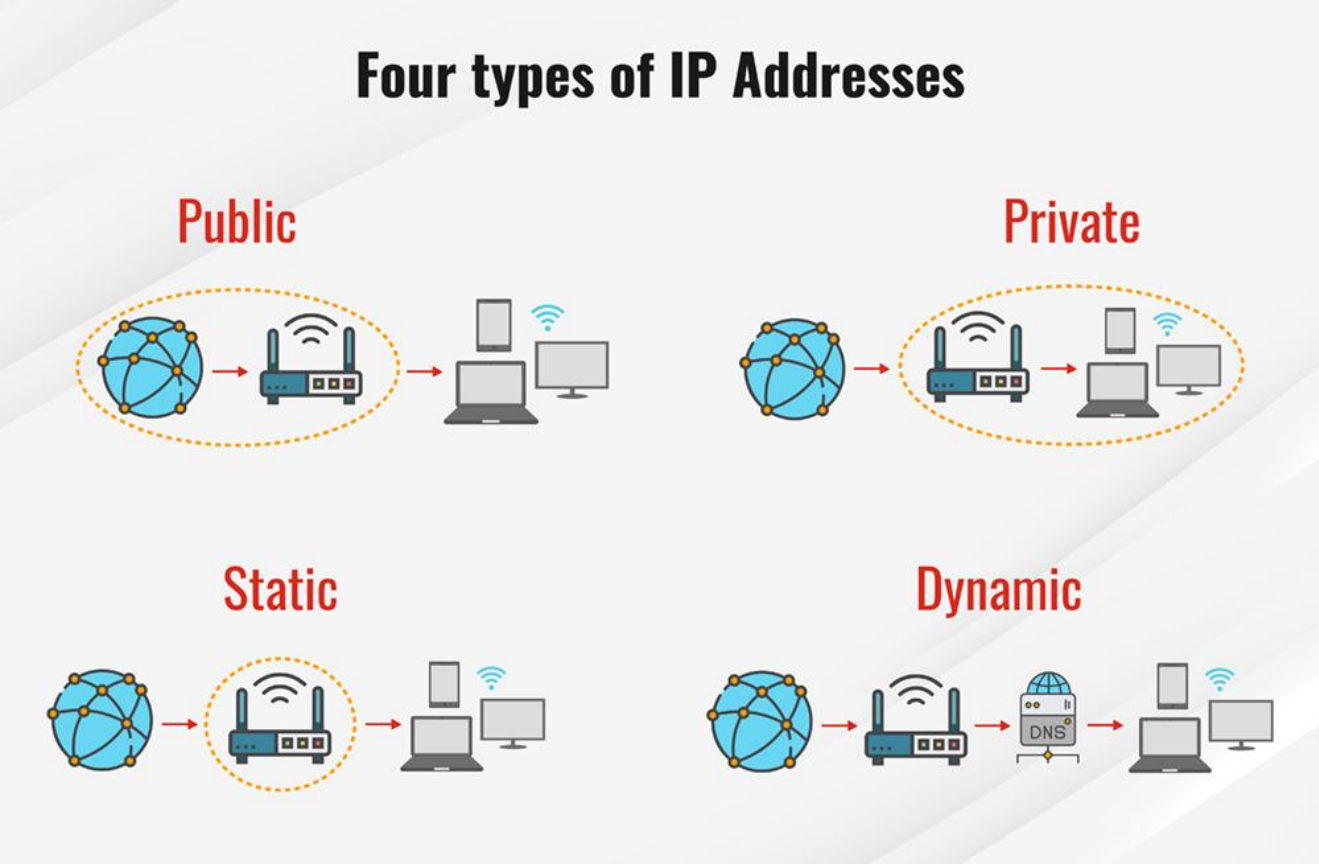
Range	Purpose
172.16.0.0 - 172.31.255.255	Private networks (Class B)
192.168.0.0 192.168.255.255	Private networks (Class C)
127.0.0.0 - 127.255.255.255	Loopback (localhost)
169.254.0.0 - 169.254.255.255	Link-local (automatic assignment)
224.0.0.0 - 239.255.255.255	Multicast
240.0.0.0 - 255.255.255.254	Experimental

https://www.geeksforgeeks.org/reserved-ip-addresses/

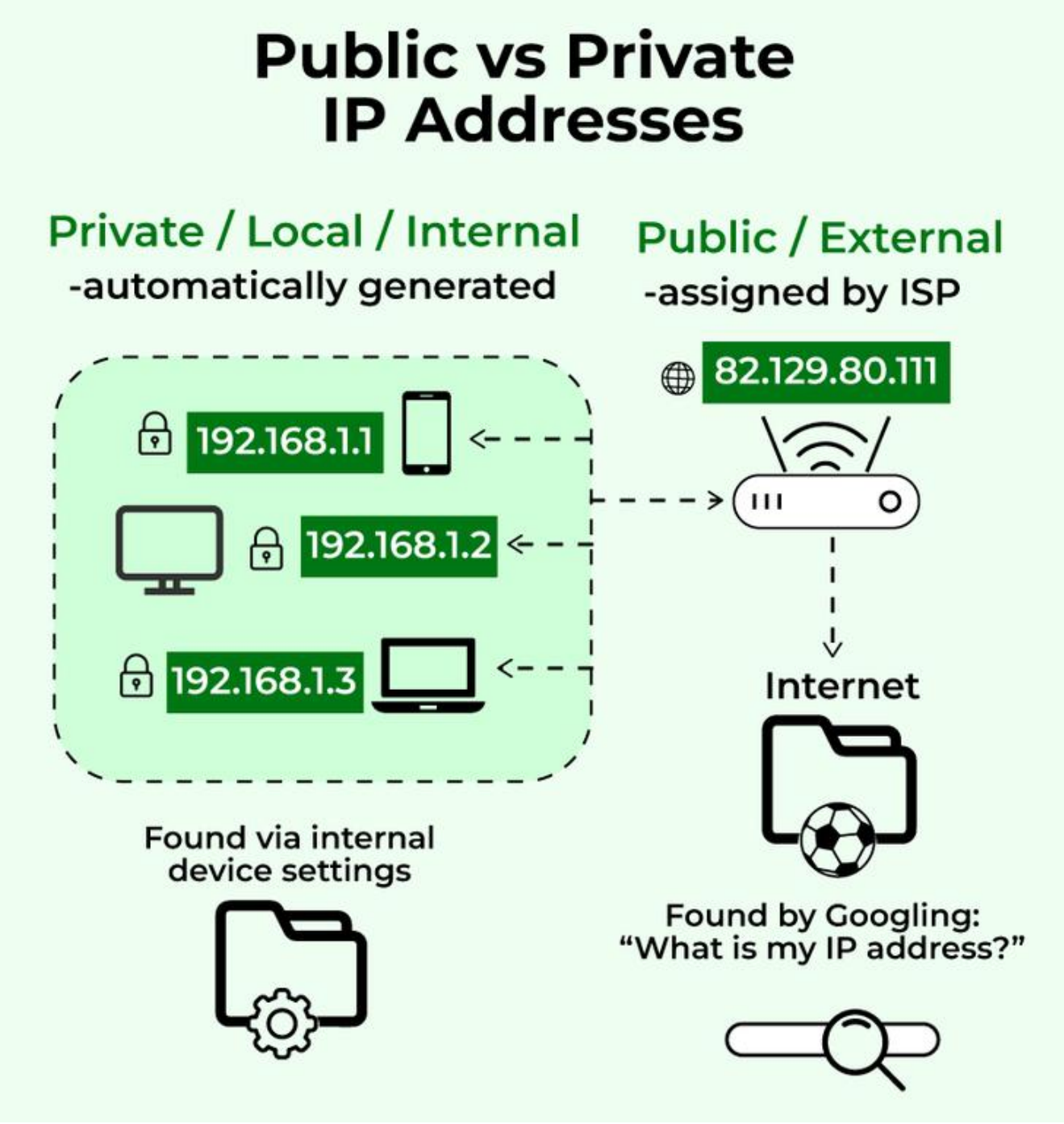
Public IP Address

https://whatismyipaddress.com/

Will show your Public IP



A public IP address is an IP address that can be accessed directly over the internet and is assigned to your network router by your internet service provider (ISP).



Public Address Ranges

- **1.0.0.0 - 9.255.255.255**
- **11.0.0.0 - 126.255.255.255**
- **129.0.0.0 - 169.253.255.255**
- **169.255.0.0 - 172.15.255.255**
- **172.32.0.0 - 191.0.1.255**
- **192.0.3.0 - 192.88.98.255**
- **192.88.100.0 - 192.167.255.255**
- **192.169.0.0 - 198.17.255.255**
- **198.20.0.0 - 223.255.255.255**

Private IP Address Ranges

- **Class A- 10.0.0.0 to 10.255.255.255**
- **Class B- 172.16.0.0 to 172.31.255.255**
- **Class C- 192.168.0.0 to 192.168.255.255**

Difference Between Private and Public IP Addresses

Private IP Address	Public IP Address
The scope of Private IP is local.	The scope of Public IP is global.
It is used to communicate within the network.	It is used to communicate outside the network.
Private IP addresses of the systems connected in a network differ in a uniform manner.	Public IP may differ in a uniform or non-uniform manner.
It works only on LAN.	It is used to get internet service.
It is used to load the network operating system.	It is controlled by ISP.
It is available free of cost.	It is not free of cost.
Private IP can be known by entering “ipconfig” on the command prompt.	Public IP can be known by searching “what is my ip” on Google.
Range: ***10.0.0.0 – 10.255.255.255,*** ***172.16.0.0 – 172.31.255.255,*** ***192.168.0.0 – 192.168.255.255***	**Range:** Besides private IP addresses, the rest are public.
Example: 192.168.1.10	Example: 17.5.7.8
Private IP uses numeric code that is not unique and can be used again	Public IP uses a numeric code that is unique and cannot be used by other
Private IP addresses are secure	The public IP address has no security and is subjected to attack

Private IP Address	Public IP Address
Private IP addresses require NAT to communicate with devices	Public IP does not require a network translation

https://www.geeksforgeeks.org/difference-between-private-and-public-ip-addresses/

Routing Calculator

https://www.calculator.net/ip-subnet-calculator.html

https://jodies.de/ipcalc

https://www.site24x7.com/tools/ipv4-subnetcalculator.html